

Analysis of Electronic Payment Systems in Ghana - A Case Study of Mobile Payment System

Regina Kafui Adzroe (Mrs)¹ Dr. Michael Asante² Francis Kwadzo Agbenyegah³

¹Head of Department (Information Communication Technology)

Hohoe E.P senior High School

² Senior Lecturer, Department of computer Science,

Kwame Nkrumah University of Science and Technology, Kumasi Ghana

³Lecturer, Faculty of Computing and Information Systems

Ghana Technology University College, Accra Ghana

Abstract:

Mobile payment is an electronic payment made through a mobile device. As the number of mobile phone subscribers in Ghana increases, so does the market for mobile money services. The majority of Ghanaians lack any formal bank account. An estimated 80 percent of Ghanaians are “unbanked” – meaning they conduct their transactions outside the banking sector with no access to financial services. Products like “mobile money,” that enable safe and secure money transfers without the use of a bank account, could have a major impact on this unserved segment of the population. Mobile money gives anyone with a mobile phone the ability to transfer money, make cash payments and conduct other financial transactions over the phone. Currently, there are four mobile money payment systems in Ghana, namely, MTN mobile money, Vodafone (VF) cash, Tigo cash and Airtel money. For an effective operation of these systems, Privacy, Traceability, Cost of Transaction, and Simplicity of the Processes involved are of much interest. The study examined the loopholes in the current mobile payment systems and proposed a framework to address the loopholes such as: Entering of information on next of kin into the system during registration, acceptance of year of birth as PIN, transactional PIN decrypted, no entering of a Valid ID number into the system, no provision for security word during token cash out, no provision for guarantor information, no provision for BoG permit number, no provision for police clearance number, and data in transit not encrypted

Keywords: Transactions, mobile money, traceability

Introduction

The world all over is witnessing an increase in electronic payment instruments to enhance the efficiency in business cycles (Abor, 2004). Bankers, technology specialists and entrepreneurs and many others over the years have continually advocated for the replacement of physical cash and the introduction of more efficient, flexible and cost effective retail payment solutions (Bank for International Settlement, 1998). With the introduction of electronic payment, all bank transactions can easily be done without going to the banking hall (Abor, 2004). To this effect, electronic payment has therefore been designed to assist all the stakeholders in minimizing problems

related to payment processes (Federal Reserve Bank of New York, 1996)

Mobile payment service (MPS) comprises the use of mobile devices such as Mobile Phone, PDA, and Wireless Tablet, connected to a Mobile Telecommunication Network, to begin a transaction; such as a purchase request, and ends a transaction by authorizing payments for the exchange of goods and services.

The use of mobile phones in such transactions makes MPS a form of electronic payment, with the exception that the transactions are carried out on the mobile phone. The vision of MPS is to transform the mobile phone into a “future wallet” holding credit card, debit account information and

mobile “cash” for transactions (Bolt, W, et. al; 2008)

Electronic retail payments continuous to emerge in Ghana to substitute or decrease paper-based payments and banks in Ghana are striving hard to catch up with the new emergence

Fundamentally, these new and emerging payment systems are based on technical innovations such as card, telephone and Internet (Abor, 2004). Some of these payments services in Ghana are Tigo cash, MTN money, Vodafone (VF) cash and Airtel money. The study therefore seeks to analyze these mobile payment systems from the viewpoints of privacy, effectiveness, processes involved, traceability and transaction cost. We shall also empirically examine the loopholes in the existing mobile payment systems in Ghana and design a framework to address the identified loopholes in the existing system. It will bring to bear the problems customers and service providers’ face in the use of the payment systems in the country for prompt measures to be taken by authorities and other stakeholders in making Ghana a cashless society.

Problem Statement

In Ghana, there has been the introduction of various payment systems which is to facilitate the exchange of transactions of either goods or services. Each payment system that has been introduced has its own benefits that it accrues to its users as well as the burdens that it poses on the customer, the merchant and the service providers of that payment system. In Ghana, the cash payment system which forms the bulk of the payments in the country involves carrying physical cash to make payments. Though, cash gives people instant purchasing power, which makes them rely on its use for their transactions, also has a carriage burden.

For instance, in order to complete a transaction involving a large sum of money the buyer needs to carry a large sum of money to the point of sales, queue up as well as spend a lot of productive hours in order to make a transaction. These bottle necks and inconveniences discourage most people, waste productive hours, and put life and resources at risk. Furthermore, the awareness of insufficient security of existing mobile payment systems owing to improper protocol design resulting in lack of vital transaction security

properties discourages merchant and their customers from using the electronic payment systems.

The study therefore seeks to analyse the mobile payment systems from the viewpoints of privacy, effectiveness, processes involved, traceability and transaction cost. It will also empirically examine the loopholes in the existing mobile payment systems in Ghana and design a framework to address the identified loopholes in the existing system.

Related Work

(Vassiliou, 2004), defines electronic payment as a form of financial exchanges that takes place between the buyer and seller facilitated by means of electronic communication. (Cobb, 2004) posits that the value of electronic payments goes way beyond the immediate convenience and safety of cards to a greater sphere of contributing to overall economic development. (Humphrey et al., 2001), on the other hand defines electronic payment as cash and related activities executed electronically. (Pariwat and Hataiseere, 2004) postulate that considerations should be given to expediency, dependability and safety of the payment method.

According to (Peirce, 2001) debit and credit cards are the most fast increasing mode of payments in any electronic transactions. (Balachandher et al., 2001) also said Telephone banking also known as telebanking is a form of artificial banking which provides financial services with the help of telecommunication devices. With this device, the customer is able to do business by dialling telephone which is linked to the bank’s system and aided by Automated Voice Response Technology. According to the authors, this speeds up productivity and the customer has an expanded access and also saves time used to visit the bank or an ATM. To (Leow, 1999) the customer gets services at their work places and in the comfort of their homes. “In Ghana, telephone banking is gaining control as most banks such as Barclays Bank, Societe General (SG) Bank all provides telephone banking. For instance “Sikatel” or SG call centre telephone banking makes it possible for clients to make enquiry relating to the bank’s products and services and also lodge complaints” (Abor, 2004).

Mobile money or mobile payment is a service in which the mobile phone is used to access financial services.

According(www.gsma.com/mobilefordevelopment/wp) mobile money_ is a convenient way for customers to establish an electronic account and maintain a 'stored value', accessible from their mobile phone, which can be used for a broad range of financial transactions. According to (Zika, 2005), a mobile payment is an electronic payment which is done with the aid of mobile device (e.g. a cell phone or a Personal Digital Assistant, PDA). Mobile payment uses a mobile device to commence and validate payment. Presently, most Banks provides active mobile banking services known as SMS Banking. SMS banking allows customers to do some banking enquires on their mobile phones without going to their banking halls. Four main components come to focus as far as mobile money is concerned. These are: Issuers (can be banks or non-bank institutions), Customers/subscribers; referred to as users who spend mobile. Money Merchant or Agents: are vendors who receive or carry out mobile money. Regulation: are defined as related authority.

Experts are of the opinion that many hurdles still needed to be cleared to progress the mobile payment system into the mainstream of electronic payment. According to (Bound J. et al., 2001) these hurdles include technology challenges as well as high up-front costs, security and enough of the right type of phone. According to researchers, security of mobile payment systems requirement can be tailored around Confidentiality (privacy), Integrity, Authorisation and Non Repudiation. According to (Bounie, and Francois, 2006) the wide acceptance of MPS is closely related to security, thus, how low the fraud rate is.

(Bound, et. Al., 2001) postulates challenges in technological advancement and the high cost of adoption to both consumers and service providers, are other challenges facing MPS as well. According to the authors, acceptance is another challenge facing MPS. Other issues according to the authors are that of compliance procedures between the banks, operators and regulatory authorities, and interoperability of the system.

According to Ghana Chamber of Telecommunications, mobile money operators in Ghana have recorded 388 mobile money fraud cases in the year 2016 as against 278 in the year 2015. This therefore represents 28.35% increase in mobile money fraud cases, an indication that mobile money fraud is on the ascendancy in Ghana. Notable among the fraud cases are

Anonymous calls from fraudsters, false promotion, Cash out fraud, Scam, False promotional SMS, False Cash out SMS, and Unauthorized PIN Access.

Methodology

The main objective of this research is to resolve the security loopholes in the current electronic payment systems i.e. mobile payment systems in Ghana. To model the electronic payment systems (mobile money systems), we design a payment platform systems using the following development resources: netbeans, JSF, Primefaces, xampp and sqlyol. We use cisco packet tracer to track data in transit in the mobile money payment platforms. To get the perception of Ghanaian community about the Mobile money payment process, a survey design is used to establish the perception of respondents in reference to mobile payment processing systems from the viewpoints of privacy, effectiveness, processes involved, traceability and transaction cost. The research incorporates all the mobile money services providers, thus, MTN, Tigo, Airtel and Vodafone as the study population. The study therefore targeted officers directly in charge of the mobile money transaction. According to the Bank of Ghana, there are currently four (4) mobile money service providers, thus informing our choice of a population size.

The researchers observed that the total population of four (4) mobile money service providers was all within reach and can conveniently be studied without necessarily making further selection. Purposive sampling was then used to select one respondent from each of the service providers sampled for the study.

Primary and secondary data constituted the sources of information for this research. Observations and interviews are used to collect the primary data. Data collected from this source focused on privacy, effectiveness, processes involved, traceability and transaction cost of the mobile money services. Secondary data on the other hand focused on registration documents and transaction charts. The tool employed for the data collection was interview. This was used to collect primary data from the officers in charge. The interview was conducted on one -on - one basis. This provided the respondents the opportunity to give a more adequate account of a peculiar phenomenon.

Microsoft office excel was then used to analyse the transaction cost vis a vis the transaction amounts. This was done in order to determine the most cost effective payment system.

Validity and Reliability of the Research Instrument

The designed framework was run several times to ensure all loopholes identified were resolved. This was done to ensure validity and reliability of the data before processing the results. Also, the researchers registered for the four mobile money services and had used them to undertake the various mobile money transactions and this gave them the first hand information through observation.

Results and Discussion

This section discussed the results of the experiment by examining the existing mobile payment processing systems and comparing it to the researcher's framework

Privacy

Analysis of the processes involved in any transaction revealed that all the four mobile payment systems make use of PIN to safeguard the subscriber's privacy and to link a subscriber or an agent to his or her account. , the use of the PIN has a deficiency in that the transaction PIN appears in plain figures which could be easily identified by a third party and thereby poses a threat to one's privacy.

Traceability

It was revealed that the mobile payment systems make use of mobile phone number, transaction ID and a valid national ID card number to track or trace transaction. It was revealed that apart from token or voucher transactions, the use of a valid ID card is not enforced by the agents. This in effect could pose a difficulty during tracking or tracing of any wrong transaction for which a valid ID card number is to be used which was earlier not registered or recorded.

Analysis of both the existing mobile payment systems and the designed framework

Registration of agents

The existing mobile payment systems in Ghana lack vital security requirements. These loopholes are:

No guarantor information is provided in the existing system: The designed framework however included the information on guarantors in order to serve as surety for the agent. This surety is expected to stand in and accepts liability in case of fraud on the part of the agents.

Figure 4.1 shows an interface of the proposed system indicating guarantors information as a mandatory field during registration by a merchant. This is mandatory as it provides an added security and reliability of information for the subscriber. The guarantor stands as a surety for the agent and therefore stands in and accepts liability in case of fraud on the part of agents

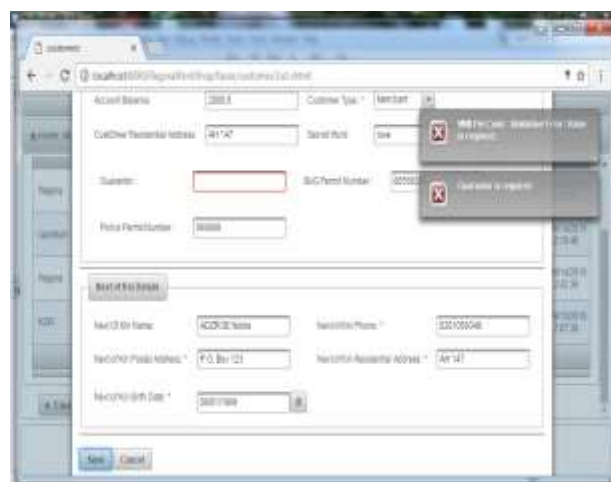


Fig. 4.1 Guarantor mandatory form

BoG permit number is not a requirement in the existing system: The designed framework resolved this lapses by ensuring BoG permit number is provided before an agent can operate any mobile money service. . Figure 4.2 displays an interface of the proposed or designed framework indicating a mandatory entering of BoG permit number by the agent. This boosts the credibility of the agent as an accredited institution whose activities are being monitored by the central bank.

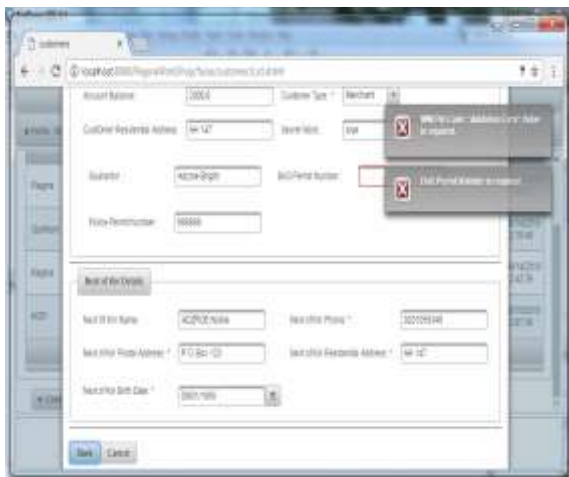


Fig. 4.2 Mandatory BoG form

Police permit number is not required in the existing system: The police permit number has been included in the designed framework. This is to serve as a clearance for the agent from any criminal record and therefore enhances the credibility of the agent. Further, it puts the operations of the agent under the watch of the security agency.

Subscriber's information during transaction

A study of the subscriber's or customers transactional processes of the existing mobile payment systems in Ghana revealed the following loopholes in the existing system.

Information on next of kin is not mandatory in the existing mobile money systems.

The current system does not ensure information on next of kin is mandatory. This is a loophole which may lead to loss of funds in the event of the death of a subscriber. A study of the existing system shows that if the next of kin information is not provided, the transaction/registration process goes on. Since the mobile money is a financial transaction, information on next of kin is vital to ensure that funds are not lost in the event of a death of a mobile account holder. The researcher therefore designed a framework to make information on next of kin a mandatory field as a prerequisite as provided in figure 4.3.



Fig.4.3 mandatory Next of Kin Forms

PIN is not encrypted in the existing system

The PIN number entered during the transaction process was not encrypted thereby compromising the security of the payment platform. The captured PIN could therefore be used to the subscriber's disadvantage and leading to payment fraud



Fig. 4.4 unencrypted PIN

The designed framework encrypts the transaction PIN in order to protect the privacy of the subscriber as well as not exposing the confidential details to a third party.

PIN encrypted: Entering of secret word is not available in the current system

The existing system does not make provision for a secret word to be asked and properly answered before token cash out transaction is accessed. This therefore

could make it possible for anyone who accidentally gets accessed to the token code to effect a transaction even though the token is not being intended for him. The designed framework makes it mandatory for a secret word to be provided by a subscriber or a non-subscriber and properly answered by a person making token cash out. This prevents fraudulent cash out, and also ensures that the right person makes out the cash out. This is illustrated in figure shown below, an interface of the proposed framework.

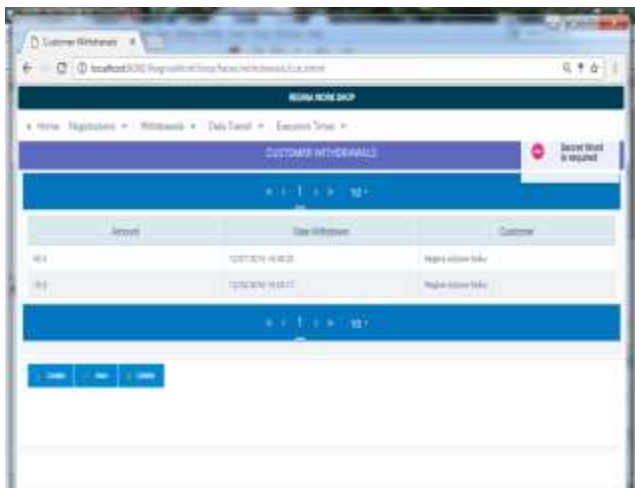


Fig 4.5 proposed framework

Interception of data in transit

Data can be intercepted in transit by any adversary who monitors the transaction processes of a mobile merchant. In the event of such interception, data is lost leading to loss of funds and loss of confidence and thereby posing serious transactional threat, credibility and traceability problems. There is therefore the need for the data in transit to be encrypted until a confirmation or feedback is received that the data reaches the intended destination. Figure 4.6 shows direct message generated by the existing system without encryption.



Fig 4.6 non – encrypted message
No encryption of data

This is evident in the fact that, when a sender makes mobile money transaction, no feedback is received by the sender to confirm whether the transaction is for the intended recipient before the message is finally delivered.

Figure 4.7 is an interface of the proposed framework that encrypted the data in transit such that even if the data is intercepted by a third party, no meaning could be made of it. In the figure 4.7, an amount of GH¢50.00 is to be transferred from the recipient to the sender. The virtual account of

the sender contains an amount of GH¢400.00 whilst that of the recipient contains no amount, thus GH¢0.00. Before the transaction is effected, the senders details are being verified and both the senders and recipients accounts are being encrypted (arrowed black and green respectively) to ensure data in transit is not intercepted. After the sender confirms and is certain of the intended recipient, both the senders as well as the recipient accounts are being decrypted (arrowed blue and red respectively) to allow the data to be accessed. Even though the current systems prompts a sender of the intended person to send the data to, sending the data at that instant could pose serious security threat to the data since between the time of identifying the recipient and sending the data, interception could take place. It is therefore expedient and safer to encrypt the data before sending to the recipient and a feedback or message is resend to the sender to further confirm the recipient before final approval for the data to be decrypted. This is to ensure that even if the data in transit is intercepted, no meaning could be made out of it. The recipient now receives a plain message of the amount sent after the sender decrypts the data. In effect, the senders virtual account is debited with GH¢50.00 (arrowed black) leaving the real account to be GH¢350.00. On the other hand, the real account of the recipient is credited with the GH¢50.00 (arrowed green) being transferred and the transaction is completed.

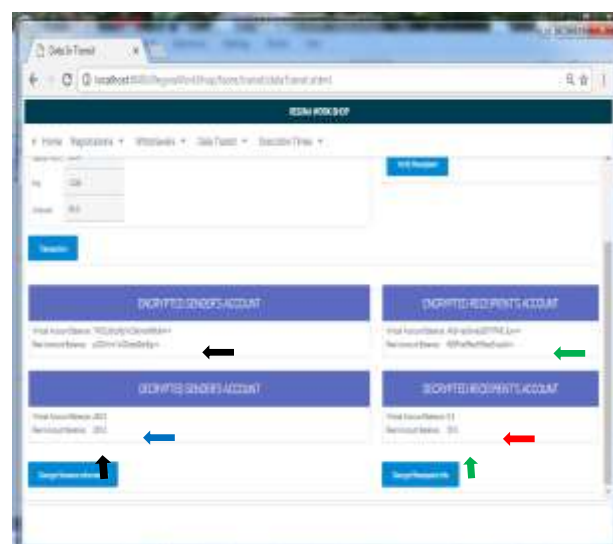


Fig 4.7 Encryption of Data in transit

CONCLUSION AND RECOMMENDATIONS

A mobile payment is an electronic payment made through a mobile device. Mobile money gives anyone with a mobile phone the ability to transfer

money, make cash payments and conduct other financial transactions over the phone. Currently, there are four mobile money service providers in Ghana, namely, MTN mobile money, VF cash, Tigo cash and Airtel money. For an effective operation of these systems, Privacy, traceability, cost of transaction, and simplicity of the processes involved are of much interest. The study therefore examined the loopholes in the current mobile money systems and a framework has been designed to resolve the loopholes.

The following loopholes have been identified, thus, Entering of information on next of kin into the system during registration is not mandatory, the current system accepts year of birth as PIN, transactional PIN is decrypted, entering of a Valid ID number into the system is not mandatory, the system does not make provision for security word or question during token cash out.

Recommendations from the study

The following recommendations from the study are worthwhile and this is expected to strengthen the mobile payment system in Ghana and also help to secure the funds of customers.

- The current mobile payment system should make it mandatory for information on next of kin to be entered during registration.
- The current mobile payment system should not accept year of birth as PIN.
- The current mobile payment system should make the transactional PIN encrypted.
- The current mobile payment system should make it mandatory for a valid ID number to be entered during withdrawals.
- The current mobile payment system should make provision for a security word during token cash out.
- The mobile money operators should improve on the efficiency of their networks to ensure reliability and also serve their customers better.
- Training should be encouraged in risk management and mobile phones security in mobile money.

References

- [1] Abor, J. (2004). Technological Innovation and Banking in Ghana, An Evaluation of Customers' Perspective. *American Academy of Financial Management*, 1(3), 338-356.
- [2] Akpaka Bruno, (2006), *Beyond the Bank: The Rise of Mobile Money in Ghana*
- [3] Annon, D. (1999). Survey of Retail Payments Systems: Consumer Payment Options Grow. *ABI/INFORM Global*, 5(4A – 13A).
- [4] Balachandher, K. G., Santha, V., Norazlin, I., & Prasad, R. (2001). Electronic Banking in Malaysia: A Note of Evolution of Services and Consumer Relations. *Journal of Internet Banking and Commerce*, 5(1), 23-37.
- [5] Bank for International Settlements, (1998), *Managing change and payment systems*, Monetary and Economic Department, no. 4, Basle
- [6] Birch, D. (1998). Purse Wars - What does the front line look like? *JIBC*.
- [7] Bolt, W., Humphrey, D. and Uittenbogaard, R. (2008). Transaction pricing and the adoption of electronic payments: A cross-country comparison, *International Journal of Central Banking* 4: 89–123.
- [8] Bound, J., Brown, C. and Mathiowetz, N. (2001). Measurement error in survey data, in J.
- [9] Heckman and E. Leamer (eds), *Handbook of Econometrics*, Elsevier Science, Amsterdam, pp. 3705–3843.
- [10] Bounie, D. and François, A. (2006). Cash, check or bank card? The effects of transaction characteristics on the use of payment instruments, *Working Paper in Economics and Social Sciences ESS-06-05*, Telecom Paris.
- [11] Brambor, T., Clark, W. R. and Golder, M. (2006). Understanding interaction models:
- [12] *Improving empirical analyses*, *Political Analysis* 14: 63– 82.
- [13] Brits, J. H. and Winder, C. (2005). Payments are no free lunch, *DNB Occasional Studies*, De Nederlandsche Bank.
- [14] Carow, K. A., & Staten, M. E. (1999). Debit, Credit, or Cash: Evidence on Gasoline Purchases. *Journal of economics and Business*, 409-421.

- [15] Chandran. (2004). Research Methods with illustrations from Christian Ministries. Nairobi: Daystar University. (n.d.).
- [16] Chorafas, D. S. (1988). Implementing Networks in Banking and Financial services. Houndmills: Macmillan Press.
- [17] Cobb Anne, (2004), <http://www.ameinfo.com/50050.html>
- [18] Costello, D. (2003., June). "Micropayment and Mobility," <http://www.epaynews.com/downloads>
- [19] Crede, A. (2004). Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems Using the Internet. Retrieved August 25, 2011, from <http://jcmc.indiana.edu/vol1/issue3/crede.html>: <http://jcmc.indiana.edu>
- [20] Duncan, T. (1998). Success of Electronic Commerce (2 nd ed.). New Jersey: John Murray Limited.
- [21] Federal Reserve Board. (2001). E-Payments in Industrial Financing. Chicago: Federal Reserve Board.
- [22] Ferguson, J. W. (2000). Electronic Commerce, Bank and Payments. 36th Annual Conference on Bank Structure Competition. Chicago, USA.
- [23] Heinrich, G., & Srinivas, G. (2001, November). <http://www.bis.org/publ/cpss48.pdf>. Retrieved September 20, 2011, from www.bis.org: <http://www.bis.org>
- [24] Humphrey, D. B., & Hancock, D. (1997). Payment Transactions, Instruments and Systems: A Survey. Journal of Banking and Finance, 21, 1573-1624.
- [25] Humphrey, D. B., Kim, M., & Vale, B. (2001). Realizing the Gains from Electronic Payments, Cost, Pricing and Payment Choice. Journal of Money, Credit and Banking, 33(2), 216-234. 66
- [26] Hunter, W. C., & Stephen, G. T. (1991). Technological Change in Large Commercial Banks. Journal of Business, 64(3), 331-362.
- [27] Jenkins, Beth, 2008, Developing Mobile Money Ecosystems, Washinton DC: IFC and Harvard
a. Kennedy School
- [28] Kenya School of Monetary Studies (KSMS), USAID, and Booz-Allen Hamilton (BAH), 2010
a. Mobile Money Transfer Services: The next phase in Evolution. Federal Reserve Bank
b. white paper.
- [29] Kichenham, B.A., Pfleeger, S.L., Pickard, L.M., Jones, P.W., Hoaglim, D.C., El Emam,
a. K., and Rosenberg, J. (2002), Preliminary Guidelines for empirical research in
b. Software Engineering, IEE Transaction on software engineering, 28,8,721-34
- [30] <http://www.computer.org/portal/web/csdl/transactions/tse.jsessionid=95acbeb01>
- [31] Kwast, Myron, Kennickell, A., (1997). Who uses electronic banking? Results from the 1995 survey of consumer finances, Mineo. Division of research and statistics, Board of Governors of the Federal Reserve System, Washington, DC, (also forthcoming in Technology, Proceedings of the 33rd Annual Conference on Bank Structure and Competition)
- [32] Leow, H. B. (1999). New Distribution Channels in Banking Services. Banker's Journal of Malaysia, 48-56.
- [33] Malek, M. (2001). E-Commerce Technologies- Electronic Payment Systems. Oslo, Norway: Steven Institute of Technology, Telecommunication Management Department.
- [34] Managing Ghana (2007), Fraud Alert Warning: Mobile Money fraud on the rise in Ghana. (<http://managingghana.com/fraud-alert-warning-mobile-money-fraud-rise-ghana/>)
- [35] Mantel, B. (2000). Why do Consumers pay Bills Electronically; An Emperical Analysis, Economic Perspective. Federal Reserve Bank of Chigago. Chigago, USA: Federal Reserve Bank of Chigago.
- [36] Metser, L. J. (2000). The Changing Nature of the Payment System: Should New Players mean New Rules? Business Review, 3-26.
- [37] Nanor, D; 2009, MTN Ghana introduces MTN mobile money. Retrieved from;

- [38] <https://techbaron.com/mtn-ghana-launches-mtn-mobile-money/>
- [39] Neuman, B. C., & Medvinsky, G. (1996). NetCheque, NetCash and the Characteristics of Internet Payments Services. *Journal of Electronic Publishing*, 2(1), 23-47.
- [40] Pariwat, S., & Hataiseree, R. (2004). The Use of Cash, Cheques and Electronic Payment Services in Thailand; Changes and Challenges for Efficiency Enhancement. *Payments Systems Group*, 73-87.
- [41] Pierce, M. (2001). Payment mechanism designed for the Internet. Retrieved 11 02, 2011, from <http://ganges.cs.tcd.ie/mepeirce/Project/oninternet.html>: <http://ganges.cs.tcd>
- [42] Smart card overview. (2006). Towards electronic money and banking: the role of Government. An introduction to electronic money issue. (1996). United States Department of the Treasury Conference. Washington DC.: United States Department of the Treasury.
- [43] Smith, C.D. (2014). Using both qualitative and quantitative research methods promotes Effectiveness. 21 March. Available at: *EzineArticles.com* <<http://ezinearticles.com/?Using-Both-Qualitative-and-Quantitative-Research-Methods-Promotes-Effectiveness-&id=1061205> (accessed on 11/06/2014).
- [44] Vartanian, P. T. (2000). *The future of electronic payments: Roadblocks and emerging practices*. London: Macmillan Press Ltd.
- [45] Vassilliou, Charalampas. (2004). *Electronic Payment system and Marketing: A literature review*. Available at: http://mis.uoa.gr/Portals/57ad7180-c5e7-49f5-b282-c6475cdb7ee7/Temple-Payment7020systems_Full%20Review/reports.
- [46] Yasuharu, U. (2003). *The Effects of Information System Investment in Banking Industry*. Kansai University.: Research Center of Socionetwork Strategies, Institute of Economic and Political Studies. Zika, J. (2005). *Retail electronic money and prepaid payment*

instruments. Prague: Institute of Economic Studies, Charles University,